PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-257816

(43)Date of publication of application : 08.10.1993

(51)Int.Cl. G06F 12/14

(21)Application number : 04-058048

(22)Date of filing : 16.03.1992

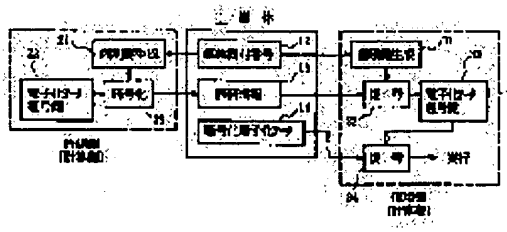
(71)Applicant : FUJITSU LTD

(72)Inventor : HASEBE TAKAYUKI
AKIYAMA RYOTA
YOSHIOKA MAKOTO

(54) ELECTRONIC DATA PROTECTION SYSTEM

(57)Abstract:

PURPOSE: To execute only software which is stored in a regular medium and permitted by giving the medium a medium characteristic number and giving the medium characteristic number the permission for the execution of the software.



CONSTITUTION: This system is provided with the medium 1 stored with ciphered electronic data 14, the medium characteristic number 12 characteristic to the medium, and permission information 13. On a permission side, a medium characteristic key based upon the medium characteristic number 12 is generated and the electronic data deciphering key for the ciphered electronic data 14 which are permitted with said medium characteristic key is ciphered and written as the permission information 13 on the medium 1. On a user side, the medium characteristic key is generated according to the medium characteristic number 12 read out of the medium 1, the read permission information 13 is deciphered with the medium characteristic key to generated the electronic data deciphering key, and the ciphered electronic data 14 are deciphered with the electronic data deciphering key to obtain the original electronic data.

LEGAL STATUS

[Date of request for examination]	12.05.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3073590
[Date of registration]	02.06.2000
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention is an electronic data protection method which protects electronic data, and relates to the electronic data protection method which prevents the unauthorized use of the software of a computer, an electronic publishing object, etc.
[0002] Generally software is easy to copy. Moreover, these illegal copy actions are performed frequently, and this obstructed the just profits of a software vendor, consequently the vicious circle that the price of software also must be set up more highly has arisen.
[0003] Moreover, it is called for that it is published briskly, the problem of copyright becomes still more important, and an electronic publishing object in recent years prevents these programs and illegal copies of data.
[0004]
[Description of the Prior Art] Conventionally, as a protection method which protects a program, an electronic publishing object, especially software, as shown in drawing 14 , there is a method which generates the consent information 72 using the user specific number 91 of a user proper. The device number (device number of the proper given to the computer) is used for this conventional method as a user specific number 91. It enciphers and software is stored in software storing data medium 71. Moreover, as consent information 72, a user's proper key is generated from the user specific number 91, the software decode key 82 is enciphered with this proper key, the consent information 72 concerned is generated, and it stores in software storing data medium 71. By receiving sale of the encryption software 73 stored in software storing data medium 71, and the consent information 72, a user decodes the encryption software 73 for the software of a plaintext, and performs this. The conventional configuration and actuation of drawing 14 are explained briefly below.
[0005] Drawing 14 shows explanatory drawing of the conventional technology. In drawing 14 , software storing data medium 71 is data medium which stores the consent information 72 which enciphered the encryption software 73 and the software decode key 82 which were enciphered, for example, a magneto-optic disk, and is data medium of the object which a user purchases from a sale side.
[0006] The consent information 72 is information which decodes the encryption software 73 and is made into the software of a plaintext, and enciphers the software decode key 82. The encryption software 73 enciphers software.
[0007] There are the individual key generation 81, the software decode key 82, an encryption circuit 83, etc. in the sale side of consent information. The individual key generation 81 generates the individual key of a user proper based on the user specific number (for example, device number) 91 of a user computer.
[0008] The software decode key 82 is a key for decoding the encryption software 73 for the software of the original plaintext. The encryption circuit 83 is a circuit which generates the consent information 72 which enciphered the software decode key 82 with the individual key of the user proper generated by the individual key generation 81.

[0009] Moreover, there are the user specific number 91, the individual key generation 92, a decoder circuit 93, the software decode key 94, a decoder circuit 95, etc. in the user computer by the side of a user. The user specific number 91 is a number of a proper which a user computer has, for example, is the device number.
[0010] The individual key generation 92 generates the individual key of a user proper based on the user specific number 91. A decoder circuit 93 decodes the consent information 72 read from purchased software storing data medium 71, and generates the software decode key 94.
[0011] The software decode key 94 is a key for decoding the encryption software 73 and decoding for the software of a plaintext. A decoder circuit 95 decodes the encryption software 73 read from software storing data medium 71 based on the software decode key 94, and makes it the software of the original plaintext. Loading of the software of this plaintext is carried out to the primary storage of a user computer, and it is performed.
[0012] Next, actuation is explained.
(1) In the consent side of consent information, the individual key generation 81 generates the individual key of a user proper based on the user specific number 91 which a user computer has. Based on this generated individual key, it writes in software storing data medium 71 by which the encryption software 73 with which the encryption circuit 83 enciphered the software decode key 82, and enciphered software as consent information 72 was stored.
[0013] (2) A user purchases software storing data medium 71 by which the consent information 72 and the encryption software 73 were written in by (1), and equips a user computer with software storing data medium 71. Based on the user specific number (for example, device number) 91 of a proper which a user computer has, the individual key generation 92 generates the individual key of a user proper. Based on the individual key of this generated user proper, a decoder circuit 93 decodes the consent information 72 read from purchased software storing data medium 71, and generates the software decode key 94. Next, a decoder circuit 95 decodes the encryption software 73 read from software storing data medium 71 based on this generated software decode key 94, and generates the software of a plaintext. Loading of the software of this generated plaintext is carried out to a primary storage, and it is performed.
[0014]
[Problem(s) to be Solved by the Invention] The user specific number 91 is used for the conventional protection method of the configuration of drawing 14 mentioned above, and the specific number of a computer or the specific number of portable hardware is usually used for it.
[0015] Since the consent information 72 will have given consent of activation to the computer and it becomes impossible to perform it only by this computer, when the specific number of a computer is used, even if it is a valid user, the problem that activation becomes impossible has arisen on a different computer. Moreover, transfer of software cannot be performed, either.
[0016] Moreover, when the specific number of portable hardware is used, the interface with the hardware itself and a computer needed to be established, and since the cost accompanying operation increases, the problem that operation becomes difficult has arisen.
[0017] This invention aims at carrying out to the ability only of the electronic data which the data-medium specific number was given to data medium of electronic data, the consent used to this data-medium specific number was given, and it was stored in data medium of normal, and consent gave being performed since these problems are solved.
[0018]
[Means for Solving the Problem] Drawing 1 shows a principle block diagram of this invention. In drawing 1 , data medium 1 stores the data-medium specific number 12 and the consent information 13 of a meaning on the enciphered encryption electronization data 14 and the data-medium proper concerned.
[0019] The individual key generation 21 and 31 generates a data-medium individual key from the data-medium specific number 12. Encryption 23 enciphers the electronic data decode key 22 with a data-medium individual key.
[0020] With a data-medium individual key, decode 32 decodes the consent information 13 and generates the electronic data decode key 33. With the electronic data decode key 33, decode 34 decodes the

encryption electronization data 14, and generates electronic data of a plaintext.
[0021]
[Function] This invention writes the encryption electronization data 14 beforehand enciphered with the data-medium specific number 12 of a meaning in data medium 1, as shown in drawing 1 . Are a consent side and the individual key generation 21 generates a data-medium proper key based on the data-medium specific number 12 of the meaning of data medium. Encryption 23 enciphers the electronic data decode key 22 with this data-medium proper key. A data-medium proper key is generated on a basis. the data-medium specific number 12 into which it writes in data medium 1 as consent information 13, and is a use side, and the individual key generation 31 read this enciphered data from data medium 1 -- The consent information 13 which decode 32 read with this data-medium proper key is decoded, the original electronic data decode key 33 is generated, the encryption electronization data 14 which decode 34 read with this electronic data decode key 33 is decoded, and it is made to make it the electronic data of a plaintext.
[0022] Moreover, an electronic data decode key 22 different every encryption electronization data 14 stored in one data medium 1 is matched. Only the electronic data decode key 22 of the encryption electronization data 14 which is a consent side and permits use is enciphered with a data-medium proper key, respectively. Only the encryption electronization data 14 corresponding to the consent information 13 which stored in data medium 1 as consent information 13, is a use side and was stored in this data medium 1 is decoded, and it is made to make it the electronic data of a plaintext.
[0023] Moreover, he is a use side and is trying to write in the data-medium specific number 12 of the meaning of a data-medium proper with the gestalt which is not rewritable. Moreover, it is a consent side, and he stores only the consent information 13 in separate data medium 1, and is trying to provide for a use side.
[0024] Moreover, it transmits to a consent information 13 use-side through a circuit from a consent side, and it is a use side, the encryption electronization data 14 is decoded from data medium 1 based on this, and it is made to make it the electronic data of a plaintext.
[0025] Moreover, he is trying to encipher the sort wear or the various data (an alphabetic character, an image, voice data, etc.) which operate a computer as encryption electronization data 14. Therefore, by giving data medium 1 which stores the encryption electronization data 14 with the gestalt which cannot rewrite the data-medium specific number 12 of a meaning, and giving the consent which uses electronic data to this data-medium specific number 12 While being able to enable use of only the encryption electronization data 14 which it was stored in data medium 1 of normal, and consent gave, transfer of the electronic data stored in data medium 1 is enabled, and it can be used, being able to load another computer with data medium 1 concerned.
[0026]
[Example] Next, the configuration and actuation of the example of this invention are explained to details using drawing 13 from drawing 2 . Here, the software used for a computer is explained to an example below as an example of the electronic data explained by drawing 1 .
[0027] Drawing 2 shows 1 example block diagram of this invention. In drawing 2 , software storing data medium 11 is data medium which stores the software which a consent side permits to a use side, for example, is data medium, such as a magneto-optic disk (disk with the capacity of hundreds of M bytes thru/or several G bytes). The data-medium specific number [not being rewritable] 12, the consent information 13 which gives consent of software to a use side, and the encryption software 15 which enciphered software are stored in this software storing data medium 11 like illustration.
[0028] The data-medium specific number 12 is a number of a meaning data-medium proper [that it is not rewritable to software storing data medium 11]. This data-medium specific number 12 is written in the field which a user cannot rewrite, and it may be made for OS to manage it, and also although it is called OS, once it writes in beforehand in the form which is not rewritable or writes in, it may be uncorrectable.
[0029] A consent side is the information which gives consent of software to a use side, and the consent information 13 is code data which decodes the encryption software 15 here (it explains in full detail

using drawing 6 and drawing 7).
[0030] The encryption software 15 enciphers software (it explains in full detail using drawing 5 from drawing 3). The individual key generation 21, the software decode key 24, encryption 23, etc. are formed in the computer by the side of consent.
[0031] The individual key generation 21 generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11 (it explains in full detail using drawing 6). Encryption 23 enciphers the software decode key 24 with the data-medium individual key generated by the individual key generation 21. This enciphered code data is stored in software storing data medium 11 as consent information 13.
[0032] The individual key generation 31, decode 32, the software decode key 35, decode 34, etc. are formed in the computer by the side of use. The individual key generation 31 generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11 (it explains in full detail using drawing 6). this -- the individual key generation 21 by the side of consent -- the same -- a data-medium individual key is generated.
[0033] With the data-medium individual key generated by the individual key generation 31, decode 32 decodes the consent information 13 read from software storing data medium 11, and generates the software decode key 35 (it explains in full detail using drawing 8).
[0034] With the software decode key 35, decode 34 decodes the encryption software 15 read from software storing data medium 11, and generates the software of a plaintext (it explains in full detail using drawing 8). Software of this generated plaintext is performed.
[0035] The configuration and actuation of drawing 2 are explained to details one by one below. Drawing 3 shows the flow chart at the time of software storing of this invention. This is a flow chart when storing in software storing data medium 11 the encryption software 15 and the enciphered consent information 13 which created software and was enciphered.
[0036] In drawing 3 , S1 creates software. This creates the software (various user programs) which a maker stores in software storing data medium. S2 creates a software cryptographic key.
[0037] S3 is matched with software and stored in a cryptographic key managed table. This is matched with the software cryptographic key managed table 4 of drawing 5 like illustration, and the software name of the software created by S1 and the cryptographic key created by S2 are stored, and it generalizes and manages it.
[0038] S4 performs ejection of the software cryptographic key corresponding to the specified software. This takes out the software cryptographic key corresponding to the software name stored in software storing data medium from the software cryptographic key managed table 4 of drawing 5 .
[0039] S5 is the software cryptographic key taken out by S4, enciphers the software of a plaintext and generates encryption software. As shown in drawing 4 , this enciphers the portion of the main part of software with an encryption key among the created software name and the main part of software, and creates a software name and the main part of encryption software like illustration. Using DES etc., **** and bit transposition are repeated and the code at this time enciphers, as explained to the lower berth.
[0040] S6 stores encryption software in storing data medium by the side of a maker. This saves the encryption software enciphered once and ejection and encryption are omitted for this saved encryption software after next time.
[0041] S7 reads encryption software and stores it in software storing data medium 11. S8 distinguishes whether the encryption software stored in software storing data medium 11 finished. In YES, it ends. In NO, sequential storing of a repeat deed and the encryption software of the directed software name is carried out for S7 at software storing data medium 11.
[0042] Above It is made the encryption software which created software and enciphered this, and this is stored in software storing data medium 11. Drawing 4 shows the example of encryption of the software of this invention.
[0043] (a) of drawing 4 shows the situation of the code of software. Here, the software name which performs a role of an identifier is stored in a header. This header is not made into the object of encryption. It considers as the object of encryption, it enciphers with an encryption key, and the main

part of software creates the main part of encryption software. The encryption at this time uses DES (Data Encryption Standerd) like illustration. This DES performs a repeat and a code for bit transposition with ****.

[0044] (b) of drawing 4 shows the situation of encryption. According to DES, like illustration, encryption enciphers with an encryption key and generates the 64-bit same bit string about a 64-bit bit string. Decode is decoded to the 64-bit original bit string with a decode key.

[0045] Drawing 5 shows the example of storing of the encryption software of this invention. In drawing 5 , the software cryptographic key managed table 4 is a table which matches the created software name and the created cryptographic key, and carries out generalization management, as mentioned already by drawing 3 . A 64-bit cryptographic key is carried out to the software name which gave "ENC" showing software being enciphered at a pair, respectively, and it stores in this software cryptographic key managed table 4.

[0046] Actuation is explained below.

(1) Take out a software cryptographic key from the software cryptographic key managed table 4 about the plaintext software which it is going to store in software storing data medium.

[0047] (2) Encipher plaintext software by the software cryptographic key to which the encryption circuit 41 was passed. Encryption is enciphered using DES of drawing 4 .

(3) Store the enciphered encryption software in software storing data medium 11 as illustration encryption software 15. It carries out repeatedly until it ends about all the plaintext software that had this specified. Under the present circumstances, what is necessary is to take out this saved encryption software from next time or subsequent ones, and just to store in software storing data medium 11, once it saves the enciphered encryption software. Moreover, the data-medium specific number 12 is a meaning number peculiar to software storing data medium 11, as mentioned already, and it is written in in the form [not being rewritable]. Moreover, the cryptographic key of the concerned cryptographic key [a decode key and] stored in the software cryptographic key managed table 4 corresponds, when an object key number is used for the algorithm of encryption.

[0048] By the above, about plaintext software, the software cryptographic key which corresponds from the software cryptographic key managed table 4 is enciphered using ejection and this, encryption software is created, and it stores in software storing data medium 11.

[0049] Drawing 6 shows the generation flow chart of the consent information on this invention. This is a flow chart which generates the consent information 13 which the software which it is going to permit enciphered, and is stored in software storing data medium 11.

[0050] In drawing 6 , S11 inputs the software name which it is going to permit. S12 picks out a software decode key from the decode key managed table 5. This picks out the decode key of the software name which is going to give consent from the software decode key managed table 5 of drawing 7 .

[0051] S13 performs ejection of a data-medium specific number. This reads the data-medium specific number of software storing data medium 11 which is going to write in consent information. S14 generates a data-medium individual key. As indicated on right-hand side, this generates the data-medium individual key enciphered with the private key about the data-medium specific number 12 of the plaintext read from software storing data medium 11, or generates the data-medium individual key enciphered with the secret algorithm about the data-medium specific number 12 of a plaintext.

[0052] With a data-medium individual key, S15 enciphers a software decode key and generates consent information. About the software decode key of a plaintext, it enciphers with the data-medium individual key generated by S14, and this generates consent information, as indicated on right-hand side.

[0053] S16 stores the enciphered consent information which was generated by S15 in software storing data medium 11. By the above, the data-medium specific number 12 is read from software storing data medium 11 which stored the encryption software 15, a data-medium individual key is generated, the consent information 13 enciphered and enciphered with this data-medium individual key about the software decode key is generated, and it stores in FUTOWEA storing data medium 11. It means that this had stored the encryption software 15 and the enciphered consent information 13 in software storing data medium 11.

[0054] Drawing 7 shows generation explanatory drawing of the consent information on this invention. In drawing 7 , in case the software decode key managed table 5 decodes the encryption software 15 and decodes it for the software of a plaintext, it matches a required software decode key with a software UEA name, and manages it. The same decode key as the software cryptographic key managed table 4 explained by drawing 5 is stored in this software decode key managed table 5. A 64-bit software decode key is stored in a pair corresponding to the software name which gave "ENC" showing being enciphered here, and each software. Actuation is explained.
[0055] (1) When selling consent information to a use side, read the data-medium specific number 12 from software storing data medium 11 first. This read data-medium specific number 12 is inputted into the individual key generation circuit 211, and a data-medium individual key is generated (S14 reference of drawing 6).
[0056] (2) Next, the software decode key of software which it is going to sell is picked out from the software decode key managed table 5, input into the encryption circuit 231, encipher with a data-medium individual key, and generate the illustration consent information 13. This consent information 13 makes a pair consent information enciphered as the software name which gave the identifier showing the enciphered purport of ENC, and stores it in software storing data medium 11 as consent information 13. Here, a software decode key and the algorithm (or private key) of the individual key generation circuit 211 protect with a safe means.
[0057] By the above, a consent side generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11, enciphers a software decode key based on this data-medium individual key, and stores it in software storing data medium 11 as consent information 13.
[0058] Drawing 8 shows the flow chart of software decode of this invention. This is a flow chart when equipping a computer with software storing data medium 11 which the use side purchased, carrying out loading of the software to a primary storage, and performing it.
[0059] In drawing 8 , S21 receives the run command of software. S22 performs ejection of the data-medium specific number 12 from software storing data medium 11.
[0060] S23 generates a data-medium individual key. This generates the data-medium individual key enciphered with the private key about the data-medium specific number 12 taken out from software storing data medium 11 by S22, as indicated on right-hand side. Or a secret algorithm generates the data-medium individual key enciphered from the data-medium specific number 12.
[0061] S24 is the data-medium individual key generated by S23, decodes the consent information 13 read from software storing data medium 11, and generates a software decode key. As indicated on right-hand side, this is the data-medium individual key enciphered by S23, decrypts the consent information 13 which is a cipher, and generates the software decode key 35 of a plaintext.
[0062] S25 reads encryption software 15 from software storing data medium 11. S26 is a software decode key, decodes the encryption software 15 read by S25, and generates the software of a plaintext. As indicated on right-hand side, about the encryption software 15 of a cipher, this is decoded with the software decode key 35 generated by S24, and generates the software of a plaintext.
[0063] S27 carries out software activation. A data-medium individual key is generated from the data-medium specific number 12 taken out from software storing data medium 11 by the above corresponding to the software run command, the consent information 13 which picked out this data-medium individual key from software storing data medium 11 on the basis is restored, the software decode key 35 is generated, the encryption software 15 taken out from software storing data medium 11 with this software decode key 35 is decoded, and the software of a plaintext is generated. It becomes possible to carry out loading of the software of this plaintext to a primary storage, and to perform it.
[0064] Drawing 9 shows explanatory drawing in the case of the program of this invention. This is explanatory drawing in the case of a program as electronic data. (a) of drawing 9 shows a whole block diagram.
[0065] In (a) of drawing 9 , a magneto-optic disk 6 is data medium which stores an encryption program etc., is equivalent to software storing data medium 11 of drawing 2 , and stores the data-medium specific

number 12, the consent information 13, and the encryption program 16. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.

[0066] At the time of program instruction activation, a program loader 61 carries out loading of the decoded program which corresponds from a magneto-optic disk 6 to a primary storage 63, changes it into the condition which can be performed, and is the processing section equipped with the key generation (individual key generation 31) mentioned already, decode (decode 32 and 34), etc. here.

[0067] A primary storage 63 is RAM (memory which can be written) for developing the program of a plaintext which the program loader 61 took out from the magneto-optic disk 6, and decoded.

[0068] Next, according to the sequence shown in the flow chart of (b) of drawing 9 , actuation of the configuration of (a) of drawing 9 is explained. In (b) of drawing 9 , S31 receives program instruction activation.

[0069] A program loader 61 finds an executive program, takes out S32, and it decodes. S33 carries out memory expansion on a primary storage. This develops on a primary storage 63 and changes into the condition that it can operate the program of a plaintext decoded by S32.

[0070] Program execution of S34 is carried out. Pro URAMU of the plaintext developed on the primary storage 63 by S33 is performed. (c) of drawing 9 shows activation explanatory drawing of the software (program) in a user computer.

[0071] (1) A user computer takes out the data-medium specific number 12 from software storing data medium 11, and generates the data-medium individual key inputted and enciphered in the individual key generation circuit 311 (S23 reference of drawing 8).

[0072] (2) About consent information 13 like the illustration taken out from software storing data medium 11, a decoder circuit 321 decodes with the data-medium individual key generated by (1), and generates a software decode key 351 (it corresponds to the software decode key 35) like illustration.

[0073] (3) About the encryption software 15 taken out from software storing data medium 11, a decoder circuit 341 decodes with the software decode key 351 generated by (2), and generates the software (program) of a plaintext. Software (program) of this plaintext is developed and performed to a primary storage 63.

[0074] Here, the encryption software 15 with which the consent information 13 is not stored cannot be decoded, and cannot be performed. Moreover, there is no data-medium specific number 12, or when software storing data medium 11 is copied to the injustice of other data medium, since it differs, the right software decode key 351 cannot be decoded from the consent information 13, and as a result, encryption software cannot be decoded for the software of a plaintext and cannot be performed. In addition, on a user computer, the algorithm of the individual key generation circuit 311 or a private key, the generated software decode key, and the decoded plaintext software protect with a safe means.

[0075] Drawing 10 shows explanatory drawing in the case of the data of this invention. This is explanatory drawing in the case of alphabetic data (text), such as data, for example, a publication etc., a mark, image data, voice data, etc. as electronic data.

[0076] (a) of drawing 10 shows a whole block diagram. In (a) of drawing 10 , a magneto-optic disk 6 is data medium which stores encryption data etc., is equivalent to software storing data medium 11 of drawing 2 , and stores the data-medium specific number 12, the consent information 13, and the encryption data 17. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.

[0077] The R/W module 64 is the processing section equipped with the key generation (individual key generation 31) which stores the decoded data which corresponds from a magneto-optic disk 6 in a primary storage 63, and mentioned it already here at the time of a lead instruction execution, decode (decode 32 and 34), etc.

[0078] A primary storage 63 is RAM (memory which can be written) for storing the data of a plaintext which the R/W module 64 picked out from the magneto-optic disk 6, and decoded. Next, according to

the sequence shown in the flow chart of (b) of drawing 10 , actuation of the configuration of (a) of drawing 10 is explained.
[0079] In (b) of drawing 10 , S41 carries out application activation. S42 executes a data reading instruction. The R/W module 64 finds data, reads and decodes S43.
[0080] S44 is stored on a primary storage. S45 performs display of data, and playback. By the above, when there is a reading instruction of data by S42, the R/W module 64 takes out and decodes the encryption data 17 from a magneto-optic disk 6, the data of a plaintext is generated, and this is stored in a primary storage 63. And it takes out from a primary storage 63, and display as a character string of a publication on a display, an image is displayed, or it generates as voice. Next, actuation of the R/W module 64 is explained to details.
[0081] (c) of drawing 10 shows display/playback explanatory drawing of the data in a user computer. (1) A user computer takes out the data-medium specific number 12 from data storage data medium 111, inputs and enciphers in the individual key generation circuit 311, and generates a data-medium individual key (S23 reference of drawing 8).
[0082] (2) About consent information 13 like the illustration taken out from data storage data medium 111, a decoder circuit 321 decodes with the data-medium individual key generated by (1), and generates a data decode key 352 (it corresponds to the software decode key 35) like illustration.
[0083] (3) About the encryption data 17 picked out from data storage data medium 111, a decoder circuit 341 decodes with the data decode key 352 generated by (2), and generates the data (alphabetic data, image data, voice data, etc.) of a plaintext. The data of this plaintext is stored in a primary storage 63, and it displays as the character string of a publication, an image, and a mark on a display, or generates as voice.
[0084] Drawing 11 shows the case where it applies to a ROM/RAM mixture mold magneto-optic disk. The magneto-optic disk of a ROM/RAM mixture mold has like illustration the field in which user rewriting is impossible, the field which can be written, and a read-only field / field only for R/W. Therefore, the data-medium specific number 12, the consent information 13, and the encryption software 15 are stored in these fields like illustration. Since this writes the data-medium specific number 12 in the field in which user rewriting is impossible, the peculiar data-medium specific number of the magneto-optic disk concerned can be given, and protection of this invention can be aimed at.
[0085] Drawing 12 shows the example in the case of storing the consent information on this invention in other storing data medium. In this case, only the data-medium specific number and encryption software of a meaning peculiar to software storing data medium are beforehand stored like illustration. And consent information is stored in another consent information storing data medium. This is an example in the case of writing beforehand a data-medium specific number and encryption software (encryption data) in data medium without the field written [CD-ROM] in, and writing the consent information which gives consent of the CD-ROMs concerned etc. in consent information storing data medium (for example, FLOPPY etc.) in which another writing is possible.
[0086] Drawing 13 shows explanatory drawing in the case of storing two or more software of this invention in data medium of one sheet. This is an example in case two or more software (or data) is stored in mass data medium (a magneto-optic disk, CD-ROM, etc.) of one sheet and carries out individual sale. In this case, software decode keys 1 and 2 ... Consent information 1 and 2 enciphered with the data-medium proper key about N, respectively ... N is generated and it stores in software storing data medium 11. And a user is the encryption software 1 and 2 stored in software storing data medium 11... If the software name of purchase hope is notified to a consent information sale side among N, it enciphers with the data-medium individual key which generated the software decode key corresponding to software from the data-medium specific number, and a consent information sale side is stored in software storing data medium 11 by making this into consent information. A user uses the encryption software which equipped with this software storing data medium 11, and was purchased by making it the software of a plaintext, decoding. On the other hand, even if a user is going to use software without consent information, he cannot decode encryption software, and he cannot use it. Moreover, since the data-medium specific number of software storing data medium 11 cannot be copied even if it copies the

consent information on other software storing data medium 11, right decode cannot be performed. This becomes possible to perform individual sale of software.

[0087]

[Effect of the Invention] Use of only the encryption electronization data 14 which according to this invention was given to data medium 1 which stores the encryption electronization data 14 with the gestalt which cannot rewrite the data-medium specific number 12 of a meaning, and it was stored in data medium 1 of normal since the configuration which gives the consent which uses electronic data to this data-medium specific number 12 had been adopted, and consent gave as explained above carries out as it is possible, and an unauthorized use can prevent. Moreover, transfer of the electronic data stored in data medium 1 is enabled, data medium 1 concerned can be used for another computer, loading, or two or more electronic data can be stored in data medium of one sheet, and individual sale can be performed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] Drawing 1 shows a principle block diagram of this invention. In drawing 1 , data medium 1 stores the data-medium specific number 12 and the consent information 13 of a meaning on the enciphered encryption electronization data 14 and the data-medium proper concerned.
[0019] The individual key generation 21 and 31 generates a data-medium individual key from the data-medium specific number 12. Encryption 23 enciphers the electronic data decode key 22 with a data-medium individual key.
[0020] With a data-medium individual key, decode 32 decodes the consent information 13 and generates the electronic data decode key 33. With the electronic data decode key 33, decode 34 decodes the encryption electronization data 14, and generates electronic data of a plaintext.

[Translation done.]

* NOTICES *

OPERATION

[Function] This invention writes the encryption electronization data 14 beforehand enciphered with the data-medium specific number 12 of a meaning in data medium 1, as shown in drawing 1 . Are a consent side and the individual key generation 21 generates a data-medium proper key based on the data-medium specific number 12 of the meaning of data medium. Encryption 23 enciphers the electronic data decode key 22 with this data-medium proper key. A data-medium proper key is generated on a basis. the data-medium specific number 12 into which it writes in data medium 1 as consent information 13, and is a use side, and the individual key generation 31 read this enciphered data from data medium 1 -- The consent information 13 which decode 32 read with this data-medium proper key is decoded, the original electronic data decode key 33 is generated, the encryption electronization data 14 which decode 34 read with this electronic data decode key 33 is decoded, and it is made to make it the electronic data of a plaintext.
[0022] Moreover, an electronic data decode key 22 different every encryption electronization data 14 stored in one data medium 1 is matched. Only the electronic data decode key 22 of the encryption electronization data 14 which is a consent side and permits use is enciphered with a data-medium proper key, respectively. Only the encryption electronization data 14 corresponding to the consent information 13 which stored in data medium 1 as consent information 13, is a use side and was stored in this data medium 1 is decoded, and it is made to make it the electronic data of a plaintext.
[0023] Moreover, he is a use side and is trying to write in the data-medium specific number 12 of the meaning of a data-medium proper with the gestalt which is not rewritable. Moreover, it is a consent side, and he stores only the consent information 13 in separate data medium 1, and is trying to provide for a use side.
[0024] Moreover, it transmits to a consent information 13 use-side through a circuit from a consent side, and it is a use side, the encryption electronization data 14 is decoded from data medium 1 based on this, and it is made to make it the electronic data of a plaintext.
[0025] Moreover, he is trying to encipher the sort wear or the various data (an alphabetic character, an image, voice data, etc.) which operate a computer as encryption electronization data 14. Therefore, by giving data medium 1 which stores the encryption electronization data 14 with the gestalt which cannot rewrite the data-medium specific number 12 of a meaning, and giving the consent which uses electronic data to this data-medium specific number 12 While being able to enable use of only the encryption electronization data 14 which it was stored in data medium 1 of normal, and consent gave, transfer of the electronic data stored in data medium 1 is enabled, and it can be used, being able to load another computer with data medium 1 concerned.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EXAMPLE

[Example] Next, the configuration and actuation of the example of this invention are explained to details using drawing 13 from drawing 2 . Here, the software used for a computer is explained to an example below as an example of the electronic data explained by drawing 1 .
[0027] Drawing 2 shows 1 example block diagram of this invention. In drawing 2 , software storing data medium 11 is data medium which stores the software which a consent side permits to a use side, for example, is data medium, such as a magneto-optic disk (disk with the capacity of hundreds of M bytes thru/or several G bytes). The data-medium specific number [not being rewritable] 12, the consent information 13 which gives consent of software to a use side, and the encryption software 15 which enciphered software are stored in this software storing data medium 11 like illustration.
[0028] The data-medium specific number 12 is a number of a meaning data-medium proper [that it is not rewritable to software storing data medium 11]. This data-medium specific number 12 is written in the field which a user cannot rewrite, and it may be made for OS to manage it, and also although it is called OS, once it writes in beforehand in the form which is not rewritable or writes in, it may be uncorrectable.
[0029] A consent side is the information which gives consent of software to a use side, and the consent information 13 is code data which decodes the encryption software 15 here (it explains in full detail using drawing 6 and drawing 7).
[0030] The encryption software 15 enciphers software (it explains in full detail using drawing 5 from drawing 3). The individual key generation 21, the software decode key 24, encryption 23, etc. are formed in the computer by the side of consent.
[0031] The individual key generation 21 generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11 (it explains in full detail using drawing 6). Encryption 23 enciphers the software decode key 24 with the data-medium individual key generated by the individual key generation 21. This enciphered code data is stored in software storing data medium 11 as consent information 13.
[0032] The individual key generation 31, decode 32, the software decode key 35, decode 34, etc. are formed in the computer by the side of use. The individual key generation 31 generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11 (it explains in full detail using drawing 6). this -- the individual key generation 21 by the side of consent -- the same -- a data-medium individual key is generated.
[0033] With the data-medium individual key generated by the individual key generation 31, decode 32 decodes the consent information 13 read from software storing data medium 11, and generates the software decode key 35 (it explains in full detail using drawing 8).
[0034] With the software decode key 35, decode 34 decodes the encryption software 15 read from software storing data medium 11, and generates the software of a plaintext (it explains in full detail using drawing 8). Software of this generated plaintext is performed.
[0035] The configuration and actuation of drawing 2 are explained to details one by one below. Drawing 3 shows the flow chart at the time of software storing of this invention. This is a flow chart when storing

in software storing data medium 11 the encryption software 15 and the enciphered consent information 13 which created software and was enciphered.
[0036] In drawing 3 , S1 creates software. This creates the software (various user programs) which a maker stores in software storing data medium. S2 creates a software cryptographic key.
[0037] S3 is matched with software and stored in a cryptographic key managed table. This is matched with the software cryptographic key managed table 4 of drawing 5 like illustration, and the software name of the software created by S1 and the cryptographic key created by S2 are stored, and it generalizes and manages it.
[0038] S4 performs ejection of the software cryptographic key corresponding to the specified software. This takes out the software cryptographic key corresponding to the software name stored in software storing data medium from the software cryptographic key managed table 4 of drawing 5 .
[0039] S5 is the software cryptographic key taken out by S4, enciphers the software of a plaintext and generates encryption software. As shown in drawing 4 , this enciphers the portion of the main part of software with an encryption key among the created software name and the main part of software, and creates a software name and the main part of encryption software like illustration. Using DES etc., **** and bit transposition are repeated and the code at this time enciphers, as explained to the lower berth.
[0040] S6 stores encryption software in storing data medium by the side of a maker. This saves the encryption software enciphered once and ejection and encryption are omitted for this saved encryption software after next time.
[0041] S7 reads encryption software and stores it in software storing data medium 11. S8 distinguishes whether the encryption software stored in software storing data medium 11 finished. In YES, it ends. In NO, sequential storing of a repeat deed and the encryption software of the directed software name is carried out for S7 at software storing data medium 11.
[0042] Above It is made the encryption software which created software and enciphered this, and this is stored in software storing data medium 11. Drawing 4 shows the example of encryption of the software of this invention.
[0043] (a) of drawing 4 shows the situation of the code of software. Here, the software name which performs a role of an identifier is stored in a header. This header is not made into the object of encryption. It considers as the object of encryption, it enciphers with an encryption key, and the main part of software creates the main part of encryption software. The encryption at this time uses DES (Data Encryption Standerd) like illustration. This DES performs a repeat and a code for bit transposition with ****.
[0044] (b) of drawing 4 shows the situation of encryption. According to DES, like illustration, encryption enciphers with an encryption key and generates the 64-bit same bit string about a 64-bit bit string. Decode is decoded to the 64-bit original bit string with a decode key.
[0045] Drawing 5 shows the example of storing of the encryption software of this invention. In drawing 5 , the software cryptographic key managed table 4 is a table which matches the created software name and the created cryptographic key, and carries out generalization management, as mentioned already by drawing 3 . A 64-bit cryptographic key is carried out to the software name which gave "ENC" showing software being enciphered at a pair, respectively, and it stores in this software cryptographic key managed table 4.
[0046] Actuation is explained below.
(1) Take out a software cryptographic key from the software cryptographic key managed table 4 about the plaintext software which it is going to store in software storing data medium.
[0047] (2) Encipher plaintext software by the software cryptographic key to which the encryption circuit 41 was passed. Encryption is enciphered using DES of drawing 4 .
(3) Store the enciphered encryption software in software storing data medium 11 as illustration encryption software 15. It carries out repeatedly until it ends about all the plaintext software that had this specified. Under the present circumstances, what is necessary is to take out this saved encryption software from next time or subsequent ones, and just to store in software storing data medium 11, once it saves the enciphered encryption software. Moreover, the data-medium specific number 12 is a

meaning number peculiar to software storing data medium 11, as mentioned already, and it is written in in the form [not being rewritable]. Moreover, the cryptographic key of the concerned cryptographic key [a decode key and] stored in the software cryptographic key managed table 4 corresponds, when an object key number is used for the algorithm of encryption.
[0048] By the above, about plaintext software, the software cryptographic key which corresponds from the software cryptographic key managed table 4 is enciphered using ejection and this, encryption software is created, and it stores in software storing data medium 11.
[0049] Drawing 6 shows the generation flow chart of the consent information on this invention. This is a flow chart which generates the consent information 13 which the software which it is going to permit enciphered, and is stored in software storing data medium 11.
[0050] In drawing 6 , S11 inputs the software name which it is going to permit. S12 picks out a software decode key from the decode key managed table 5. This picks out the decode key of the software name which is going to give consent from the software decode key managed table 5 of drawing 7 .
[0051] S13 performs ejection of a data-medium specific number. This reads the data-medium specific number of software storing data medium 11 which is going to write in consent information. S14 generates a data-medium individual key. As indicated on right-hand side, this generates the data-medium individual key enciphered with the private key about the data-medium specific number 12 of the plaintext read from software storing data medium 11, or generates the data-medium individual key enciphered with the secret algorithm about the data-medium specific number 12 of a plaintext.
[0052] With a data-medium individual key, S15 enciphers a software decode key and generates consent information. About the software decode key of a plaintext, it enciphers with the data-medium individual key generated by S14, and this generates consent information, as indicated on right-hand side.
[0053] S16 stores the enciphered consent information which was generated by S15 in software storing data medium 11. By the above, the data-medium specific number 12 is read from software storing data medium 11 which stored the encryption software 15, a data-medium individual key is generated, the consent information 13 enciphered and enciphered with this data-medium individual key about the software decode key is generated, and it stores in FUTOWEA storing data medium 11. It means that this had stored the encryption software 15 and the enciphered consent information 13 in software storing data medium 11.
[0054] Drawing 7 shows generation explanatory drawing of the consent information on this invention. In drawing 7 , in case the software decode key managed table 5 decodes the encryption software 15 and decodes it for the software of a plaintext, it matches a required software decode key with a software UEA name, and manages it. The same decode key as the software cryptographic key managed table 4 explained by drawing 5 is stored in this software decode key managed table 5. A 64-bit software decode key is stored in a pair corresponding to the software name which gave "ENC" showing being enciphered here, and each software. Actuation is explained.
[0055] (1) When selling consent information to a use side, read the data-medium specific number 12 from software storing data medium 11 first. This read data-medium specific number 12 is inputted into the individual key generation circuit 211, and a data-medium individual key is generated (S14 reference of drawing 6).
[0056] (2) Next, the software decode key of software which it is going to sell is picked out from the software decode key managed table 5, input into the encryption circuit 231, encipher with a data-medium individual key, and generate the illustration consent information 13. This consent information 13 makes a pair consent information enciphered as the software name which gave the identifier showing the enciphered purport of ENC, and stores it in software storing data medium 11 as consent information 13. Here, a software decode key and the algorithm (or private key) of the individual key generation circuit 211 protect with a safe means.
[0057] By the above, a consent side generates a data-medium individual key based on the data-medium specific number 12 read from software storing data medium 11, enciphers a software decode key based on this data-medium individual key, and stores it in software storing data medium 11 as consent information 13.

[0058] Drawing 8 shows the flow chart of software decode of this invention. This is a flow chart when equipping a computer with software storing data medium 11 which the use side purchased, carrying out loading of the software to a primary storage, and performing it.
[0059] In drawing 8 , S21 receives the run command of software. S22 performs ejection of the data-medium specific number 12 from software storing data medium 11.
[0060] S23 generates a data-medium individual key. This generates the data-medium individual key enciphered with the private key about the data-medium specific number 12 taken out from software storing data medium 11 by S22, as indicated on right-hand side. Or a secret algorithm generates the data-medium individual key enciphered from the data-medium specific number 12.
[0061] S24 is the data-medium individual key generated by S23, decodes the consent information 13 read from software storing data medium 11, and generates a software decode key. As indicated on right-hand side, this is the data-medium individual key enciphered by S23, decrypts the consent information 13 which is a cipher, and generates the software decode key 35 of a plaintext.
[0062] S25 reads encryption software 15 from software storing data medium 11. S26 is a software decode key, decodes the encryption software 15 read by S25, and generates the software of a plaintext. As indicated on right-hand side, about the encryption software 15 of a cipher, this is decoded with the software decode key 35 generated by S24, and generates the software of a plaintext.
[0063] S27 carries out software activation. A data-medium individual key is generated from the data-medium specific number 12 taken out from software storing data medium 11 by the above corresponding to the software run command, the consent information 13 which picked out this data-medium individual key from software storing data medium 11 on the basis is restored, the software decode key 35 is generated, the encryption software 15 taken out from software storing data medium 11 with this software decode key 35 is decoded, and the software of a plaintext is generated. It becomes possible to carry out loading of the software of this plaintext to a primary storage, and to perform it.
[0064] Drawing 9 shows explanatory drawing in the case of the program of this invention. This is explanatory drawing in the case of a program as electronic data. (a) of drawing 9 shows a whole block diagram.
[0065] In (a) of drawing 9 , a magneto-optic disk 6 is data medium which stores an encryption program etc., is equivalent to software storing data medium 11 of drawing 2 , and stores the data-medium specific number 12, the consent information 13, and the encryption program 16. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.
[0066] At the time of program instruction activation, a program loader 61 carries out loading of the decoded program which corresponds from a magneto-optic disk 6 to a primary storage 63, changes it into the condition which can be performed, and is the processing section equipped with the key generation (individual key generation 31) mentioned already, decode (decode 32 and 34), etc. here.
[0067] A primary storage 63 is RAM (memory which can be written) for developing the program of a plaintext which the program loader 61 took out from the magneto-optic disk 6, and decoded.
[0068] Next, according to the sequence shown in the flow chart of (b) of drawing 9 , actuation of the configuration of (a) of drawing 9 is explained. In (b) of drawing 9 , S31 receives program instruction activation.
[0069] A program loader 61 finds an executive program, takes out S32, and it decodes. S33 carries out memory expansion on a primary storage. This develops on a primary storage 63 and changes into the condition that it can operate the program of a plaintext decoded by S32.
[0070] Program execution of S34 is carried out. Pro URAMU of the plaintext developed on the primary storage 63 by S33 is performed. (c) of drawing 9 shows activation explanatory drawing of the software (program) in a user computer.
[0071] (1) A user computer takes out the data-medium specific number 12 from software storing data medium 11, and generates the data-medium individual key inputted and enciphered in the individual key generation circuit 311 (S23 reference of drawing 8).

[0072] (2) About consent information 13 like the illustration taken out from software storing data medium 11, a decoder circuit 321 decodes with the data-medium individual key generated by (1), and generates a software decode key 351 (it corresponds to the software decode key 35) like illustration.
[0073] (3) About the encryption software 15 taken out from software storing data medium 11, a decoder circuit 341 decodes with the software decode key 351 generated by (2), and generates the software (program) of a plaintext. Software (program) of this plaintext is developed and performed to a primary storage 63.
[0074] Here, the encryption software 15 with which the consent information 13 is not stored cannot be decoded, and cannot be performed. Moreover, there is no data-medium specific number 12, or when software storing data medium 11 is copied to the injustice of other data medium, since it differs, the right software decode key 351 cannot be decoded from the consent information 13, and as a result, encryption software cannot be decoded for the software of a plaintext and cannot be performed. In addition, on a user computer, the algorithm of the individual key generation circuit 311 or a private key, the generated software decode key, and the decoded plaintext software protect with a safe means.
[0075] Drawing 10 shows explanatory drawing in the case of the data of this invention. This is explanatory drawing in the case of alphabetic data (text), such as data, for example, a publication etc., a mark, image data, voice data, etc. as electronic data.
[0076] (a) of drawing 10 shows a whole block diagram. In (a) of drawing 10 , a magneto-optic disk 6 is data medium which stores encryption data etc., is equivalent to software storing data medium 11 of drawing 2 , and stores the data-medium specific number 12, the consent information 13, and the encryption data 17. This magneto-optic disk 6 is purchased from a consent side, and optical-magnetic disc equipment is equipped with it. Besides this magneto-optic disk 6, you may be storages, such as an optical disk, CD-ROM, FD and HD, a magnetic tape, and a cassette tape.
[0077] The R/W module 64 is the processing section equipped with the key generation (individual key generation 31) which stores the decoded data which corresponds from a magneto-optic disk 6 in a primary storage 63, and mentioned it already here at the time of a lead instruction execution, decode (decode 32 and 34), etc.
[0078] A primary storage 63 is RAM (memory which can be written) for storing the data of a plaintext which the R/W module 64 picked out from the magneto-optic disk 6, and decoded. Next, according to the sequence shown in the flow chart of (b) of drawing 10 , actuation of the configuration of (a) of drawing 10 is explained.
[0079] In (b) of drawing 10 , S41 carries out application activation. S42 executes a data reading instruction. The R/W module 64 finds data, reads and decodes S43.
[0080] S44 is stored on a primary storage. S45 performs display of data, and playback. By the above, when there is a reading instruction of data by S42, the R/W module 64 takes out and decodes the encryption data 17 from a magneto-optic disk 6, the data of a plaintext is generated, and this is stored in a primary storage 63. And it takes out from a primary storage 63, and display as a character string of a publication on a display, an image is displayed, or it generates as voice. Next, actuation of the R/W module 64 is explained to details.
[0081] (c) of drawing 10 shows display/playback explanatory drawing of the data in a user computer. (1) A user computer takes out the data-medium specific number 12 from data storage data medium 111, inputs and enciphers in the individual key generation circuit 311, and generates a data-medium individual key (S23 reference of drawing 8).
[0082] (2) About consent information 13 like the illustration taken out from data storage data medium 111, a decoder circuit 321 decodes with the data-medium individual key generated by (1), and generates a data decode key 352 (it corresponds to the software decode key 35) like illustration.
[0083] (3) About the encryption data 17 picked out from data storage data medium 111, a decoder circuit 341 decodes with the data decode key 352 generated by (2), and generates the data (alphabetic data, image data, voice data, etc.) of a plaintext. The data of this plaintext is stored in a primary storage 63, and it displays as the character string of a publication, an image, and a mark on a display, or generates as voice.

[0084] Drawing 11 shows the case where it applies to a ROM/RAM mixture mold magneto-optic disk. The magneto-optic disk of a ROM/RAM mixture mold has like illustration the field in which user rewriting is impossible, the field which can be written, and a read-only field / field only for R/W. Therefore, the data-medium specific number 12, the consent information 13, and the encryption software 15 are stored in these fields like illustration. Since this writes the data-medium specific number 12 in the field in which user rewriting is impossible, the peculiar data-medium specific number of the magneto-optic disk concerned can be given, and protection of this invention can be aimed at.
[0085] Drawing 12 shows the example in the case of storing the consent information on this invention in other storing data medium. In this case, only the data-medium specific number and encryption software of a meaning peculiar to software storing data medium are beforehand stored like illustration. And consent information is stored in another consent information storing data medium. This is an example in the case of writing beforehand a data-medium specific number and encryption software (encryption data) in data medium without the field written [CD-ROM] in, and writing the consent information which gives consent of the CD-ROMs concerned etc. in consent information storing data medium (for example, FLOPPY etc.) in which another writing is possible.
[0086] Drawing 13 shows explanatory drawing in the case of storing two or more software of this invention in data medium of one sheet. This is an example in case two or more software (or data) is stored in mass data medium (a magneto-optic disk, CD-ROM, etc.) of one sheet and carries out individual sale. In this case, software decode keys 1 and 2 ... Consent information 1 and 2 enciphered with the data-medium proper key about N, respectively ... N is generated and it stores in software storing data medium 11. And a user is the encryption software 1 and 2 stored in software storing data medium 11... If the software name of purchase hope is notified to a consent information sale side among N, it enciphers with the data-medium individual key which generated the software decode key corresponding to software from the data-medium specific number, and a consent information sale side is stored in software storing data medium 11 by making this into consent information. A user uses the encryption software which equipped with this software storing data medium 11, and was purchased by making it the software of a plaintext, decoding. On the other hand, even if a user is going to use software without consent information, he cannot decode encryption software, and he cannot use it. Moreover, since the data-medium specific number of software storing data medium 11 cannot be copied even if it copies the consent information on other software storing data medium 11, right decode cannot be performed. This becomes possible to perform individual sale of software.

[Translation done.]